[redacted]

e/e PAID SWLing

National Security Agency—the organization which directs America's super-secret communications intelligence efforts, these intercept posts eavesdrop on the radio and radar transmissions of both friendly and not-so-friendly nations.

Ever Listening. While current fiction interest centers around spy and super-spy, more meaningful intelligence data in real life comes from listening. Reason is that when collected in large enough quantities and properly analyzed, radio transmissions can tell much about a country's strengths and weaknesses.

To gain insight into how a large, dry-land monitor post operates, we spoke to an Army sergeant who had been stationed at one near Asmara, Eritrea.

"The station's antenna farm is located on top of a nearby plateau," he told us. "Head-end amplifiers boost the signals from these antennas and pass them on via trunk feeders. Splitters at the station divide the signals among individual receivers." Typical of these couplers are the CU-168s now showing up on the surplus market.

The sergeant added other details. "At Fort Monmouth, New Jersey, I had been taught to copy Cyrillic (i.e., the Russian) alphabet CW on an electric typewriter—I never learned to *send* code. We were amazed at how much Soviet traffic was sent by key CW," he revealed. "We'd listen in to tanks on maneuvers talking to each other and their headquarters on 3 to 4 MHz CW!"

This dependence on manual Morse has led to doubts about Russia's man-in-space program, since few conventional SWLs have heard Soviet Cosmonauts. But had these listeners turned on the BFOs (and been able to copy Russian CW), they might have heard the 20- and 42-MHz signals of the orbiting brass pounders. For the truth is that Uncle Sam's monitors *have* listened in on every Soviet space shot, including some which literally never got off the ground.

Site 23. One of the posts intercepting Russian space radio traffic is simply called Site 23. Located near the village of Golbasi, south of Ankara, Turkey, the station functions in a manner similar to the Asmara installation just mentioned.

According to descriptions, creature comforts at Site 23 rate high. Both bachelor and family quarters for some 800 persons are available. Entertainment facilities include a pool, clubs, tennis courts, and similar accommodations provided at military posts having more prosaic missions.

While the exact duties of Site 23 are top secret, it's believed the post played a key role in the communications network for U-2 flights operated over the Soviet Union (these were discontinued after Francis Gary Powers was shot down and taken prisoner in 1960). Originally staffed by U.S. personnel, Site 23 is now run by Turks trained in the United States.

On the other side of the world, at a monitor post on Clark Field in the Philippines and at others in arctic Alaska, GI operators who fluently understand one or more Chinese dialects—but who may not be able to speak the language—translate voice, CW, and teletypewriter radio communications.

Counterintelligence operations also man intercept posts to trap those very few espionage agents who communicate with their headquarters by radio. When contacting its agents, Moscow has favored 6340; 8888; 14,775; and 17,080 kHz, with 8888 more a calling than a working frequency. Other channels employed usually lie near international broadcast bands.

Burp Transmissions. Can ordinary SWLs eavesdrop on these transmissions? It's all but impossible, since messages are sent in 240 wpm CW—each sounds like a burst of static or a burp. Agents using two two-speed tape recorders drop this machine-gun paced code to a reasonable speed, then decipher its five-letter word groups. What some SWLs have reported as secret spy instructions quite probably were nothing more than stock market reports or details of shady business deals.

Ultimately, all messages picked up by government monitors are passed on through intelligence channels to the headquarters of the National Security Agency at Ft. Meade, Maryland. There, computers break even the toughest codes and ciphers. Traffic-analysis techniques identify military units and attempt to establish their conditions of readiness.

Not all radio monitoring work is so dramatic. One of the missions of the Central Intelligence Agency is listening to foreign broadcast stations. CIA posts all over the world pick up and pass on to Washington details of every major program. Daily, a special staff edits, correlates, prints, and issues this information to the agency's "customers." The subject of a broadcast might be important; so, too, might be what was left unsaid. And, as former CIA chief Allen Dulles admitted, resident CIA agents have occasionally scooped news bulletins.

This activity was most recently illustrated when CIA and U.S. State Department monitors were first to learn of the surprise invasion of Czechoslovakia by Warsaw Pact nations. On the evening of August 20, these government SWLs picked up R. Prague's BCB outlets announcing the border crossings. Later that night, many conventional SWLs heard the early close-down of Prague's shortwave outlet following its transmissions to South America. Russian mechanized units rolled into the city as the last strains of the [illegible] were heard on the 7345 kHz channel.

How It Began. Electronic eavesdropping had its origin early in World War I. In 1915, a British Army Intelligence listening post was intercepting German field orders transmitted in plain text from a powerful spark set in Berlin. By the end of the war, accurate radio direction finding had been developed and great progress had been made in codes and ciphers.

During the early 20s, U.S. Army Signal Corps intercept posts helped genius codebreaker Herbert Yardley crack secret messages from several foreign nations. More than once during international negotiations his efforts gave U.S. representatives valuable insights into the other side's thinking. Yardley's so-called black chamber was closed in 1929 when the then Secretary of State Henry L. Stimson flatly stated, "Gentlemen do not read each other's mail."

The Navy also realized the value of monitoring the airwaves. By 1926 it had, among others, a station on the fourth floor of the American consulate in Shanghai, China. When its regenerative receivers could not pick up short-range transmissions from Japanese warships at sea, several sets were installed aboard the destroyer U.S.S. *McCormick*. That autumn, the ship became the first floating monitor post, secretly eavesdropping on Japanese fleet exercises.

During the 1930s, the Army and Navy operated listening posts in the continental U.S., Panama Canal Zone, Hawaii, Puerto Rico, and on Corregidor in the Philippines. Through an unofficial arrangement sometimes hampered by red tape and snafus, these stations supplied William F. Friedman of the Signal Corps with the hundreds of messages which enabled him to break the Japanese Purple Code. Friedman, using mathematical permutations derived from the intercepts, constructed a Purple machine functionally the same as those used by the Japanese.

In Europe during World War II, the Germans maintained extensive listening networks, backed by direction finding and cryptoanalysis facilities to trap spies and saboteurs. They intercepted several Roosevelt-Churchill transatlantic radiotelephone conversations using de-scrambling equipment.

Luftwaffe monitors backed up Reich radar defenses. According to post-war interviews, by listening to "ramp checks" of SCR-274N transmitters aboard Eighth Air Force bombers, the number of aircraft and often the target of upcoming raids could be determined. The Japanese used similar tactics and maintained a huge intercept station in the southern home islands. From its receivers came information which helped Japan plan its strategic and tactical defense.

Counterattack! With extensive use of radar came countermeasures to block its all-seeing eye. Specialized equipment extended the military SWL's frequency coverage to several thousand megahertz. Airborne APR-type UHF receivers and ARA scope read-out analyzers were developed to determine the

continued